



Information Technology Security Management (ITSM) Services

Expense Recovery

**Methodology and
Approved Fee Schedule**

Table of Contents

Table of Contents.....2

Executive Summary3

Information Technology Security Management Services4

 Incident Management4

 Risk Management.....5

Information Technology Security Management Services Fee Coverage6

Cost Recovery Methodology.....7

Information Technology Security Management (ITSM) Service Fee

 Calculation7

Executive Summary

The General Assembly of the Commonwealth of Virginia has mandated several new Security functions. The expenses for these mandated services must be recovered through the use of Internal Service Funds. A new fee, to be called the Information Technology Security Management (ITSM) Service Fee, is being created for cost recovery related to the new responsibilities that have been assigned to the Security Services Directorate.

This document outlines the new Security services as they relate to the new ISF recovery requirement. The calculation of the fees necessary to recover the expenses is also detailed.

The recovery target for the Information Technology Security Management (ITSM) Service Fee is \$3,450,813. This includes a VITA administrative charge. The ITSM fee to all VITA in-scope agencies for Security Services is based on the number of PCs and other devices, but will be billed to agencies as a lump-sum on a monthly basis. The fee will be \$51.67 per eligible device, per year or \$4.31 per month. Eligible devices include Desktop PCs, Laptop PCs, and Tablet PCs. The fee will be calculated annually.

The ITSM Fee has been reviewed and approved by the VITA Management, the Information Technology Investment Board (ITIB), the Joint Legislative Audit and Review Commission (JLARC) Internal Service Fund Rate Subcommittee, and by JLARC itself. The effective date for the ITSM Service Fee is June 1st, 2006.

Information Technology Security Management Services

Providing a combined information technology (IT) infrastructure for the Commonwealth requires a robust enterprise-wide Information Technology Security Management program. Previously, each agency maintained its own IT infrastructure, and decisions on types and levels of security in each agency typically did not affect other agencies. In a shared IT infrastructure, however, each agency is exposed to the same information technology risks and information security incidents as every other agency that uses the infrastructure and the infrastructure is only as strong as its “weakest link”.

Providing effective information asset protection in this environment requires, therefore, that VITA provide enterprise-wide IT Security Management services that protect all agencies, guarding against any weak links. Such protection is particularly critical in the areas of Incident Management and Risk Management, the specific program areas funded by the IT Security Management fee. This fee will fund services, detailed below, that are not funded in Security Services’ current budget. The total recovery target for this fee is \$3,450,813. This includes a VITA administrative charge.

The ITSM Fee has been reviewed and approved by the VITA Management, the Information Technology Investment Board (ITIB), the Joint Legislative Audit and Review Commission (JLARC) Internal Service Fund Rate Subcommittee, and by JLARC itself. The effective date for the ITSM Service Fee is July 1st, 2006.

Incident Management

Services provided under this category include:

- Development of Incident Management policies, standards, processes, and procedures
- Collection and management of information security incidents across the VITA enterprise
- Forensic analysis of information security incidents collected
- Enterprise-wide anticipation of, response to, and eradication of information security incidents
- Increased protection of confidentiality, integrity, and availability of Commonwealth information assets commensurate with their criticality and sensitivity

Risk Management

Services provided under this category include:

- Development and implementation of policies and standards for risk analysis and risk mitigation strategies..
- Oversight and coordination of Code-mandated database and data communications audits
- Increased protection of the combined IT infrastructure, based on up-to-date analyses of individual and collective Agency business requirements

Enterprise-wide Information Security Incident and Risk Management are critical to effective information asset protection. The IT Security Management Fee will provide additional consistent, cost-effective, enterprise-wide management of the information technology infrastructure needed to protect the Commonwealth's information assets and to enable VITA's customer agencies to serve their customers effectively.

The following page details the Incident and Risk Management services that the IT Security Management Fee will cover.

Information Technology Security Management Services Fee Coverage

Service Area	ITSM Fee Covers	ITSM Fee does not Cover
Incident Management		
<ul style="list-style-type: none"> • Development of Incident Management policies, standards, processes, and procedures 	<ul style="list-style-type: none"> • Development of policies, standards, processes, and procedures related to Incident Management 	<ul style="list-style-type: none"> • Development of Enterprise IT Security policies, standards, processes, and procedures
<ul style="list-style-type: none"> • Collection and management of security information across the VITA enterprise 	<ul style="list-style-type: none"> • Collection and management of data from collection points strategically sited according to risk 	<ul style="list-style-type: none"> • Instrumentation and collection of security data from all points in the Enterprise
<ul style="list-style-type: none"> • Forensic analysis of information collected 	<ul style="list-style-type: none"> • Forensic analysis of relevant information 	<ul style="list-style-type: none"> • Forensic analysis of all information collected
<ul style="list-style-type: none"> • Enterprise-wide proactive preparation for, response to, and eradication of information security incidents 	<ul style="list-style-type: none"> • Proactive preparation for, response to, and eradication of security incidents in the VITA-managed Enterprise, including coordination with Institutions of Higher Education 	<ul style="list-style-type: none"> • Management of security incidents outside the VITA-managed Enterprise; fee does not cover management of incidents for Institutions of Higher Education
<ul style="list-style-type: none"> • Increased protection of confidentiality, integrity, and availability of Commonwealth information assets commensurate with their criticality and sensitivity 	<ul style="list-style-type: none"> • Information security incident management functions that protect critical and sensitive data and systems from information security incidents 	<ul style="list-style-type: none"> • Information security management functions that provide coverage independent of criticality and sensitivity
Risk Management		
<ul style="list-style-type: none"> • Evaluation of Agency IT requirements to determine IT infrastructure requirements to support critical business processes 	<ul style="list-style-type: none"> • Development of Risk Management policies, standard, and guidance; evaluation of Agency IT requirements 	<ul style="list-style-type: none"> • Development of Agency BIAs and RAs
<ul style="list-style-type: none"> • Development and maintenance of an enterprise-wide IT infrastructure Risk Assessment, based on Agency and VITA's IT requirements 	<ul style="list-style-type: none"> • Development of enterprise-wide IT infrastructure Risk Assessment 	<ul style="list-style-type: none"> • Development of Agency application Risk Assessments
<ul style="list-style-type: none"> • Development and implementation of enterprise-wide risk mitigation strategies based on the enterprise-wide IT infrastructure Risk Assessment 	<ul style="list-style-type: none"> • Development and implementation of enterprise-wide infrastructure risk mitigation strategies 	<ul style="list-style-type: none"> • Development and implementation of risk mitigation strategies for Agency applications
<ul style="list-style-type: none"> • Oversight and coordination of Code-mandated database and data communications audits 	<ul style="list-style-type: none"> • Coordination and oversight of database and data communications audits; technical vulnerability scanning and penetration testing; auditing where no other audit mechanism exists; annual reporting. 	<ul style="list-style-type: none"> • Development of Agency audit plans; auditing of all databases and data communications
<ul style="list-style-type: none"> • Increased protection of the combined IT infrastructure, based on up-to-date analyses of individual and collective Agency IT requirements 	<ul style="list-style-type: none"> • Risk management functions that provide adequate protection for the IT infrastructure 	<ul style="list-style-type: none"> • Risk management intended specifically to protect individual Agency applications

Incident Management Items identified as not covered by the ITSM Fee are unfunded, except for development of Enterprise IT Security policies, standards, procedures, etc., which is covered by the existing Security Services budget, and management of incidents for Institutions of Higher Education, which is the responsibility of the Institutions, themselves. Risk Management items identified as not covered by the ITSM Fee are Agency responsibilities.

Cost Recovery Methodology

The ITSM fee to all VITA in-scope agencies for Security Services is calculated based on the number of PCs and other devices, but will be billed to agencies as a lump-sum on a monthly basis. The fee will be \$51.67 per eligible device, per year or \$4.31 per month. Eligible devices include Desktop PCs, Laptop PCs, and Tablet PCs. The fee will be calculated annually. The table below shows the calculated fee based on the 2006 Fiscal Year Budget for the VITA Security Services Directorate.

Information Technology Security Management (ITSM) Service Fee Calculation

Total Eligible Devices:	66,789
Recovery Target (Direct Expense)	\$3,270,293
Administrative Charge (Indirect Expense)	<u>\$180,520</u>
Total Amount to Recover	\$3,450,813
Calculated Annual Fee:	\$51.67
Monthly Charge:	\$4.31